

DEVICE AND MEDIA CONTROLS PROCEDURE

The Department of Mental Health (DMH) must implement security safeguards that govern the receipt and removal of hardware and electronic media that contain electronic Information into and out of a facility, and the movement of these items within the facility.

1. Receipt of hardware and software into a facility.
 - A. The System Managers/Owners must maintain a secured record documenting all hardware and software received into the facility.
 - B. The System Managers/Owners must document all hardware and software according to access, clearance levels, and/or data set type, as needed.
 - C. The System Managers/Owners must scan the components (e.g., software, storage devices) for malicious software.
 - D. The System Managers/Owners must create a backup of any software received, and securely store the backup until the software is no longer in use.
 - E. The System Managers/Owners must provide an accounting of all documentation to DMH Chief Information Officer (CIO) at the time of receipt of the hardware and/or software.
2. Removal of hardware and software from a facility.
 - A. The System Managers/Owners or designee must first give written approval before any hardware or software is removed from a facility.
 - B. The System Managers/Owners must consider the reasons for the requested removal of any hardware and software and must consider:
 1. The requestor's access and clearance levels.
 2. The requestor's job requirements.
 3. Sensitivity of the components.
 4. The period and/or frequency of removal.
 - C. The System Managers/Owners must document all requests and decisions concerning removal of any hardware and software.
 - D. The System Managers/Owners must update the hardware and software inventory system for both the removal and return of any hardware and software.
 - E. The System Managers/Owners must inspect any hardware and software upon its return to the facility, including performing a scan for malicious software.
 - F. The System Managers/Owners must provide an accounting of all documentation to the DMH CIO at the time of the removal and return of the hardware and/or software.

3. Data Backup

- A. The System Managers/Owners must determine when backups are required before the movement of any hardware and software.
- B. If a backup is created, it shall be made in accordance with the data backup processes in the DMH Policy 550.03, Information Technology Contingency Plan Policy.
- C. Any backup created must be tested to ensure that the copy is exact and is retrievable.
- D. Any backup created must be stored in a secure location with appropriate access controls in place.

4. Disposal of hardware and software

- A. The System Managers/Owners must ensure that the hardware and software inventory system is appropriately updated upon the disposal of the hardware and/or software.
- B. Before disposal, the System Managers/Owners must ensure that all Protected Health Information (PHI) and other confidential and/or sensitive information on any component are irreversibly destroyed. The System Managers/Owners must verify and document that the sanitization steps have been completed.
- C. The System Managers/Owners must remove any labeling that had been affixed to the component before its disposal and affix it to the disposal documents.
- D. The System Managers/Owners must provide an accounting of all documentation to the DMH CIO at the time of the sanitization of the hardware and/or software.
- E. Each System Managers/Owners must submit written documentation with the disposal documents to verify that the sanitization steps were completed.

5. Reuse of Devices and Media

- A. The System Managers/Owners must ensure that the hardware and software inventory system is appropriately updated upon the reallocation of components.
- B. Prior to reuse, the System Managers/Owners must ensure all information on any component that is not necessary to the job function of the person to whom it is being reassigned is irreversibly destroyed. The System Managers/Owners must verify and document that the sanitization steps have been completed.

6. Accountability

- A. The System Managers/Owners must maintain a record of the movement of hardware, software, electronic media and devices, and of the persons responsible for those components.

- B. The System Managers/Owners may use existing inventory systems to collect the information required by this procedure. In the absence of an inventory system, facilities must develop appropriate systems to collect the required information.
- C. The System Managers/Owners must ensure that the hardware and software inventory system is up-to-date and secured.